CHAPTER 11

ANTI-SPAM SERVERS FOR WINDOWS

In previous chapters, we've talked a lot about client anti-spam tools and how they are great for individual users. But what about tools for the organization? The logical chokepoint for spam is at the mail gateway, and since most organizations do not run UNIX-based e-mail solutions, we offer the following Windows-based server solutions.

IHATESPAM SERVER EDITION

Why not start with the tool whose name says how we all really feel about spam? If you think we already covered this product in Chapter 10, you're only half correct. In addition to a client tool, Sunbelt Software also distributes a server-based anti-spam tool. Like the client version, iHateSpam Server Edition is a multistrategy spam fighter using semantic and rules-based filtering and black/whitelists to block spam at the mail gateway. Out of the box, iHateSpam claims a 90 percent or better accuracy rate, although we had a considerably lower percentage on initial install.

iHateSpam runs on Windows 2000 Server with Service Pack 3 or later and MS Exchange 2000 with Service Pack 3 or later. iHateSpam Server Edition is a commercial program distributed either on CD or as a download from Sunbelt Software's web site at *http://www.sunbelt-software.com*. The base install allows for 25 mailboxes, with additional "packs" of mailboxes available for purchase separately.

How It Works

iHateSpam controls spam at the gateway by applying word-based and rules-based filters, blacklists, and whitelists either globally (to all e-mail accounts) or by policies (to one or groups of e-mail accounts). While both rules and e-mail lists are customizable, Sunbelt Software provides a regularly updated ruleset that covers most of the spam strategies out there. Mail that hits its spam rules are assigned a "spam probability," and if the administrator-definable threshold is reached, the mail is either deleted or pushed to a user-accessible quarantine folder for review. Additionally, iHateSpam has a powerful reporting engine that builds regular spam reports and stores them in an Access database file (included) or SQL file.

Installing iHateSpam

iHateSpam should be installed on the Windows server running Exchange. As stated previously, iHateSpam is distributed either as a single installation file from the Sunbelt Software web site or via CD. We installed the downloaded version on a Windows 2000 Server running Exchange 2000.

Preinstall Checklist

Other than the system requirements, you must have Administrator access to the machine where you wish to install iHateSpam. If you wish to install the Reporting facilities for MSSQL (either SQL 2000 or MSDE 2000), you must have SQL installed and running and mixed mode authentication turned on. Refer to SQL, Windows, and iHateSpam documentation for more information on using SQL with iHateSpam.

Installing

To install iHateSpam Server Edition on Windows, perform these steps:

1. Log in to your Windows server as Administrator or as user with Administrator rights.
2. Double-click the installation file, and the initial splash window appears.
3. Click Next. The Welcome screen appears.
4. Click Next. The User Information window appears, as shown in Figure 11-1.
5. Enter your name and your organization's name, and choose who will have access to the program. (We suggest you choose the Only For Me radio button for security reasons.) Then click the Next button.
6. At the License Agreement window, click the I Agree radio button and then click Next.
7. In the Destination Folder window, select an install directory. We suggest the default (*$Windowsroot*\SunbeltSoftware\iHateSpam Server Edition\), unless you have some other policy regarding program installation on your server. Click the Next button when you're ready.
8. The Select Features window allows you to install either the Server Components or Standalone Report Viewer (or both). For this install, leave it set at the default, which is both, and click Next.
9. The Ready window allows you to click Back if you want to change any of the settings or click Cancel to cancel the install. Click Next when you've pondered all that could go wrong and you decide to go ahead anyway.
10. After iHateSpam installs, the Installation Utility Object window appears, as shown in Figure 11-2. Here you can set up the database management system where iHateSpam stores its reports. The default is a Microsoft Access database called iHateSpamDB.MDB. You can configure iHateSpam to write to an SQL database (which it also creates) by clicking the Database Settings button. (See the "Preinstall Checklist" section for more information about enabling iHateSpam for SQL reporting.) Click Reporting Enabled to enable reporting, and then click the Done button.
11. The Exchange 2000 Event Sink Setup window opens. This window offers one checkbox for each instance of the Exchange SMTP service you're running on Exchange and two buttons: Install SMTP Sink and Cancel, as shown in Figure 11-3. Check each instance listed and click the Install SMTP Sink button to register iHateSpam with each service.
12. After you click the Install SMTP Sink button, a confirmation window appears, letting you know how many sinks have been registered successfully. Click OK, and the main Event Sink Setup window reappears, listing all instances of SMTP registered (the checkboxes should be grayed out now). Click OK to finish the initial configuration.

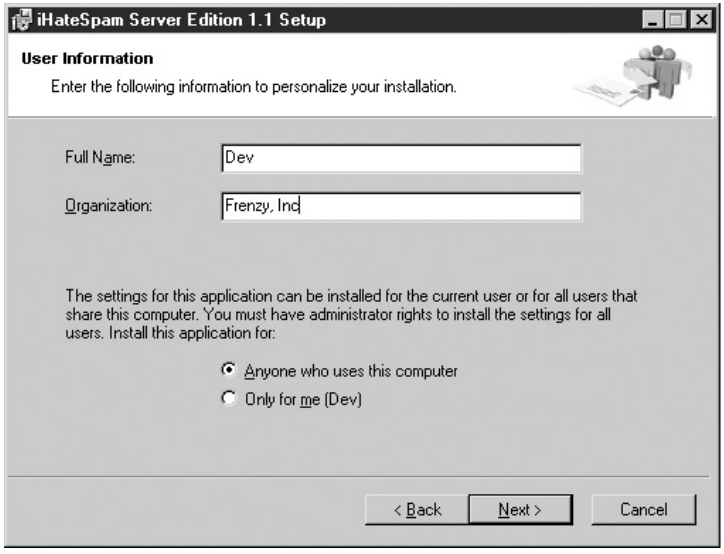

iHateSpam Server Edition 1.1 Setup
User Information
Enter the following information to personalize your installation.
Full Name:
Dev
Organization:
Frenzy, Inc
The settings for this application can be installed for the current user or for all users that share this computer. You must have administrator rights to install the settings for all users. Install this application for:
Anyone who uses this computer
Only for me (Dev)
< Back
Next >
Cancel

Figure 11-1. The User Information Window

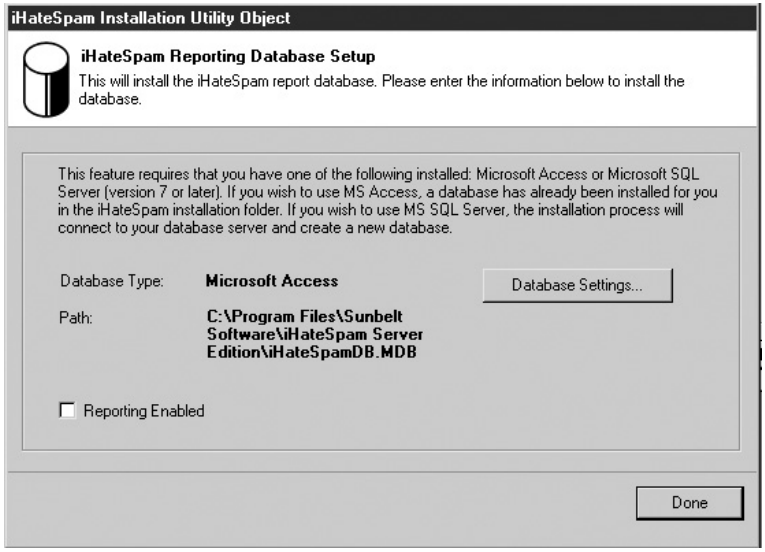

iHateSpam Installation Utility Object
iHateSpam Reporting Database Setup
This will install the iHateSpam report database. Please enter the information below to install the database.
This feature requires that you have one of the following installed: Microsoft Access or Microsoft SQL Server (version 7 or later). If you wish to use MS Access, a database has already been installed for you in the iHateSpam installation folder. If you wish to use MS SQL Server, the installation process will connect to your database server and create a new database.
Database Type:
Microsoft Access
Database Settings...
Path:
C:\Program Files\Sunbelt Software\iHateSpam Server Edition\iHateSpamDB.MDB
Reporting Enabled
Done

Figure 11-2. The Installation Utility Object window

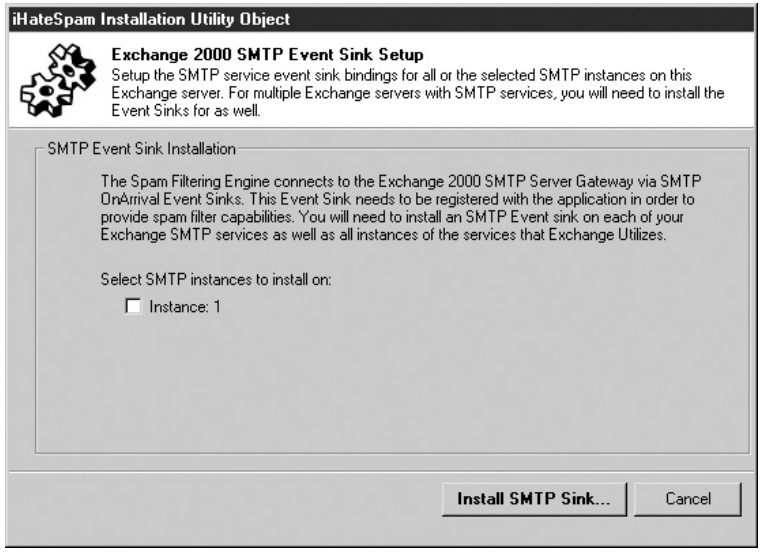

iHateSpam Installation Utility Object
Exchange 2000 SMTP Event Sink Setup
Setup the SMTP service event sink bindings for all or the selected SMTP instances on this Exchange server. For multiple Exchange servers with SMTP services, you will need to install the Event Sinks for as well.
SMTP Event Sink Installation
The Spam Filtering Engine connects to the Exchange 2000 SMTP Server Gateway via SMTP OnArrival Event Sinks. This Event Sink needs to be registered with the application in order to provide spam filter capabilities. You will need to install an SMTP Event sink on each of your Exchange SMTP services as well as all instances of the services that Exchange Utilizes.
Select SMTP instances to install on:
Instance: 1
Install SMTP Sink...
Cancel

Figure 11-3. The Exchange 2000 Event Sink Setup window

13. A window proclaiming success appears. Click the Finish button, and iHateSpam prompts you to restart.

Exchange SMTP OnArrival Sink

iHateSpam uses the Exchange SMTP OnArrival Sink to scan incoming e-mail. This function communicates the incoming e-mail message, along with the transport envelope fields, to iHateSpam for rules processing. You don't really have to know how the SMTP sink works, since iHateSpam configures and registers itself for communication with Exchange, but be sure to check each Instance listed on the Exchange 2000 SMTP Sink Window (Figure 11-3). If you're curious, a very thorough description of SMTP/NNTP sinks and other Collaboration Data Objects (CDO) COM components appears on Microsoft's MSDN site at *http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cdosys/html/_cdosys_smtp_nntp_transport_event_sinks_with_cdo.asp*.

Hating Spam in the Enterprise

Straight out of the box, iHateSpam does nothing for you. You have to configure it to get mail and apply its rules and policies. iHateSpam creates a shortcut on your desktop, but you can also access the management console by navigating to Start | Programs | iHateSpam Server Edition | iHateSpam Server Edition Manager. The iHateSpam management console appears, as shown in Figure 11-4.

To access the main management console window, click the iHateSpam Server Edition folder in the left pane. The right pane populates with big, friendly icons: Management, Spam Filtering, Reporting, About, Help, and Registration. Clicking any of these icons allows you to access the various functions described in the following sections. You may also navigate the management functions through the folder tree in the left pane, and you can always access the Help window by pressing the F1 key.

Management The Management group gives you access to both User and System Management configuration options.

User Management The User Management tool allows you to set policies for each individual user as well as disable filtering entirely per user. The User Management tool provides a search function, as well as a list of preconfigured searches, as shown in Figure 11-5.

To assign a policy to a user, enter the user's mailbox/username in the User Search field and click the Search button. The user appears in a table detailing his or her e-mail address,

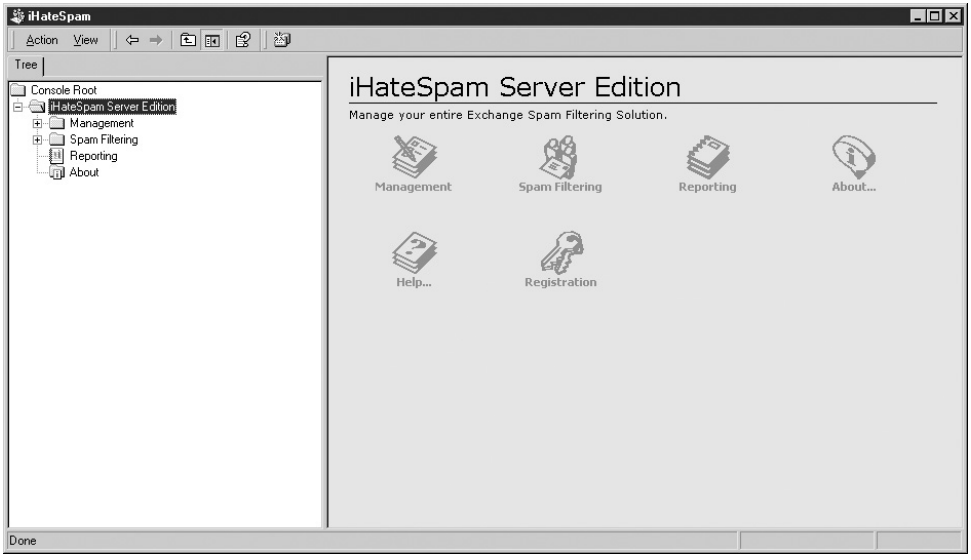


Figure 11-4. The iHateSpam management console

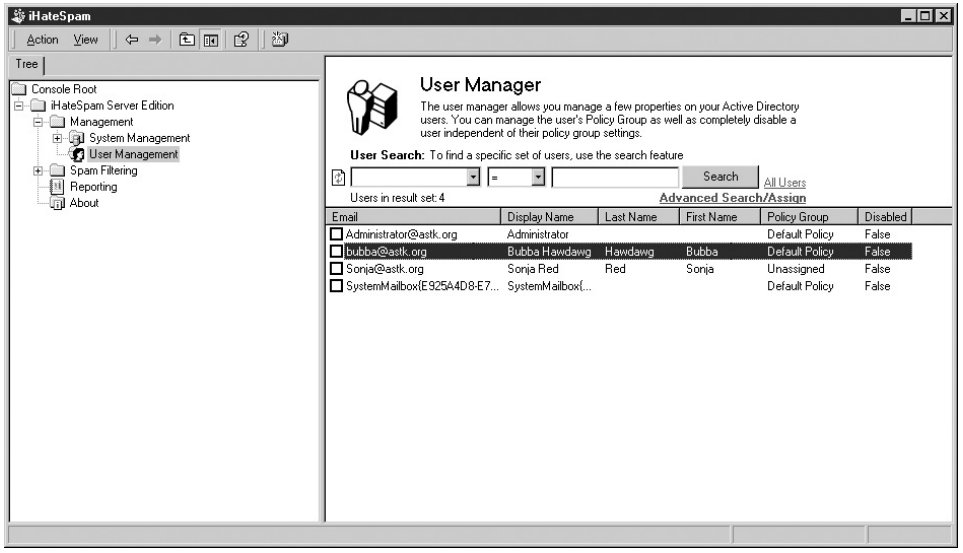
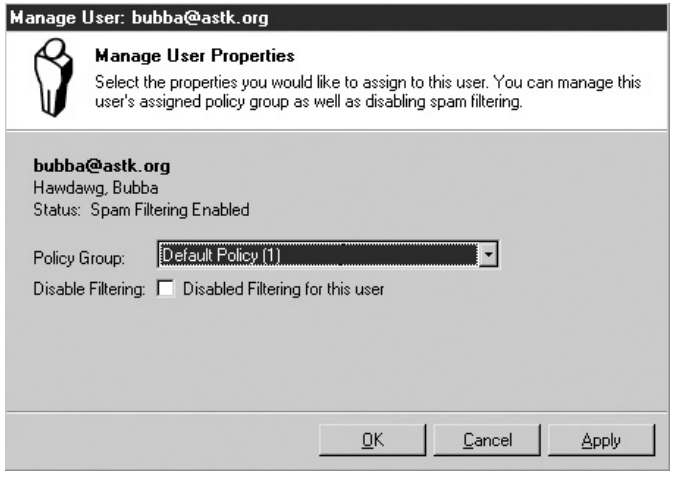


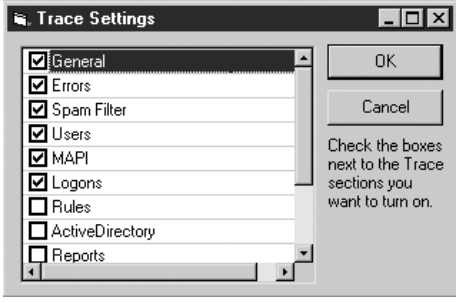
Figure 11-5. The User Management tool

display name, first and last name, Policy Group applied (default is Unassigned), and Disabled status (default is False). Double-click the username, and the Manage User window appears, as shown here. Select the policy you want to apply from the Policy Group drop-down and, if desired, disable filtering by clicking the Disabled Filtering checkbox (if desired). Click the OK button. Since only the Default Policy is available right now, we'll talk more about assigning user policies in the "Spam Filtering: Policies" section.


Manage User: bubba@astk.org
Manage User Properties
Select the properties you would like to assign to this user. You can manage this user's assigned policy group as well as disabling spam filtering.
bubba@astk.org
Hawdawg, Bubba
Status: Spam Filtering Enabled
Policy Group:
Default Policy (1)
Disable Filtering:
Disabled Filtering for this user
OK
Cancel
Apply

System Management If you click the System Management icon from the main management console, you'll see another console view with the following functionality: General Settings, Reporting, Registration, SMTP Event Bindings, Smart Caching, Replication, and Domain Configuration.

The General Settings window allows you to turn spam filtering on and off and also allows you to configure iHateSpam for Tracing Mode. Tracing Mode records all iHateSpam events to various trace or log files. This mode is used for troubleshooting problems, but click the Settings button now. A Trace Settings window appears, as shown next. Simply check the events you wish to log and click the OK button. Then, click the On radio button to enable Trace Mode.



NOTE Trace Mode is used for tracking down problems, such as mail bottlenecks and other specific errors. iHateSpam in Trace Mode quickly generates very large log files. It's recommended, therefore, that you use this mode only if you need to troubleshoot a problem.

The Reporting icon (or the Reporting folder in the System Management tree) brings up the System Management: Reporting Settings window, as shown in Figure 11-6. This window should already be populated, as configured during the installation, with the Database Type (default: Microsoft Access), Path (default: $RootProgramFiles\Sunbelt Software\iHateSpam Server Edition\iHateSpamDB.MDB), and the Reporting Enabled checkbox checked. If this is not the case, click the Install/Configure Reporting button and the default settings should populate the fields. Check the Reporting Enabled checkbox, and then click the Done button. The settings should populate the fields in the Reporting Settings window.

Smart Caching is an iHateSpam feature that holds user, policy configuration, and filtering information in a cache to increase the performance of the filtering engine. The cache updates automatically on regular intervals. The Smart Caching window displays the Current Status (default: Smart Caching Enabled) and provides a button that you can click to clear/reset the cache. Normally, this isn't necessary, but if you make changes to user policies, filters, or other configuration information, you should clear the cache to apply the settings immediately.

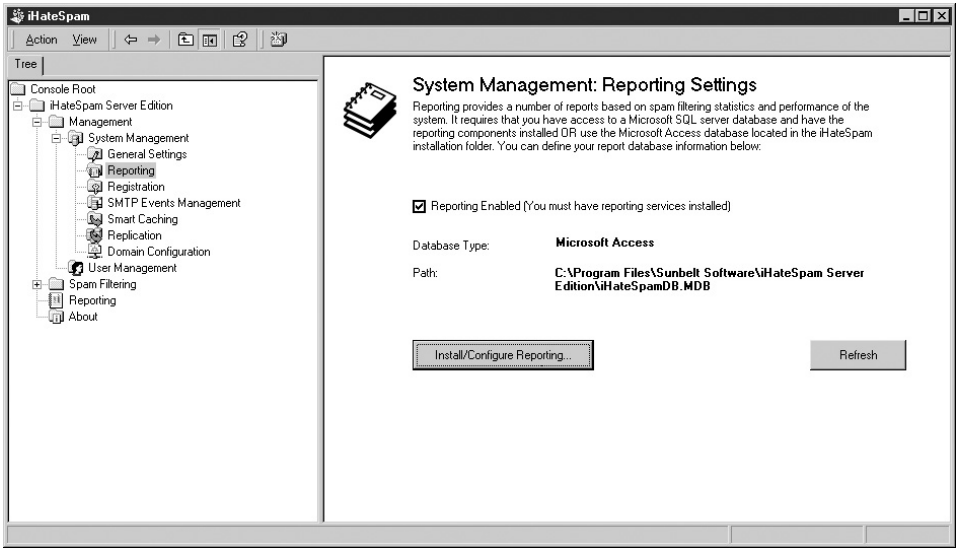

iHateSpam
Action View
Tree
Console Root
iHateSpam Server Edition
Management
System Management
General Settings
Reporting
Registration
SMTP Events Management
Smart Caching
Replication
Domain Configuration
User Management
Spam Filtering
Reporting
About
System Management: Reporting Settings
Reporting provides a number of reports based on spam filtering statistics and performance of the system. It requires that you have access to a Microsoft SQL server database and have the reporting components installed OR use the Microsoft Access database located in the iHateSpam installation folder. You can define your report database information below:
Reporting Enabled (You must have reporting services installed)
Database Type:
Microsoft Access
Path:
C:\Program Files\Sunbelt Software\iHateSpam Server Edition\iHateSpamDB.MDB
Install/Configure Reporting...
Refresh

Figure 11-6. Reporting Settings window

TIP Are your rules not working? Receiving spam from a recently added blacklist domain? Go to the Smart Caching window, clear the cache, and test again.

The Replication management window, shown in Figure 11-7, allows you to add Exchange servers for centralized iHateSpam administration. To add an Exchange server, click the Add Server button. The Add Replication Server window appears (see Figure 11-8), where you can type the Server Name and the UNC Path to the iHateSpam installation folder in the appropriate fields. Click the OK button to save it. To remove a server, select the server in the Available Servers table of the Replication management window, and then click the Remove button.

NOTE You must add the proper SMTP sinks and domains (discussed in the section "Installing") for iHateSpam to work correctly on more than one server. This assumes that the access permissions between the various servers are properly configured as well.

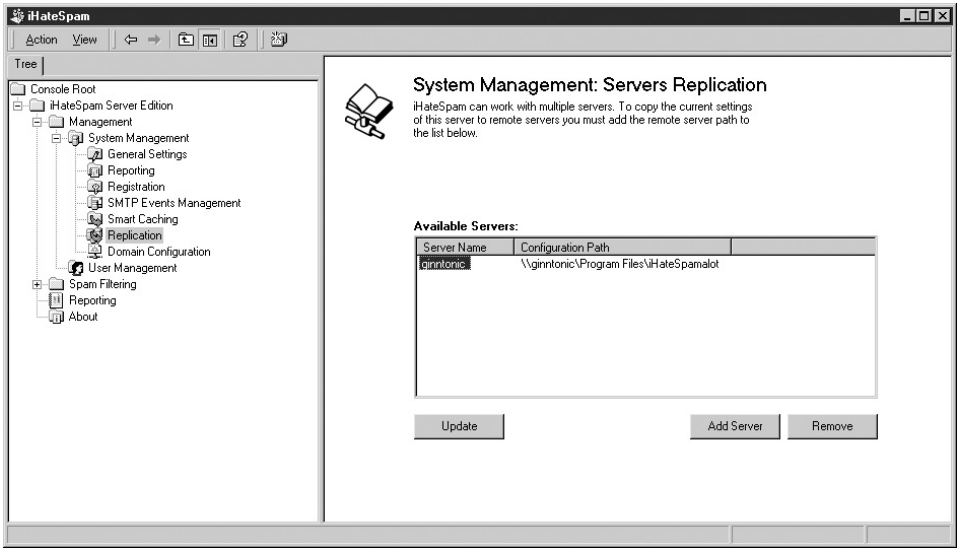


Figure 11-7. Replication management window

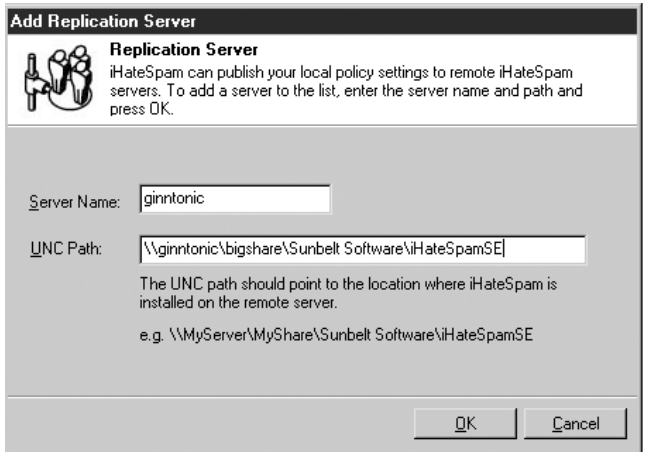

Add Replication Server
Replication Server
iHateSpam can publish your local policy settings to remote iHateSpam servers. To add a server to the list, enter the server name and path and press OK.
Server Name:
ginntonic
UNC Path:
\\ginntonic\bigshare\Sunbelt Software\iHateSpamSE
The UNC path should point to the location where iHateSpam is installed on the remote server.
e.g. \\MyServer\MyShare\Sunbelt Software\iHateSpamSE
OK
Cancel

Figure 11-8. Add Replication Server window

The Domain Configuration window allows you to query user accounts (filter mail for them) on all the domains available to you. In most cases, you will not have to bother with this window. iHateSpam automatically populates this table with the appropriate domains (based on the SMTP sinks you configured during installation). However, if you manage many domains and you want iHateSpam to filter on only a few of them, pull up this window and uncheck those domains you don't wish to query for users. Again, this should not be necessary, since you probably didn't add the SMTP sink for those unwanted domains in the first place. Of course, if you happen to add a domain with an Exchange server to your wide-area network (WAN), you'll have to add the SMTP sink (discussed in the following paragraph). The domain itself will populate automatically in this case.

The SMTP Events Management window and the Registration window are rarely used. As discussed in the preceding paragraph, if you add another Exchange server, you will have to go to the SMTP Events management window and bind an SMTP sink to that server if you want to filter spam for its users. The Registration window allows you to register your software with iHateSpam. Simply enter your Registration Key and Number Of Seats in the appropriate fields and click the Register button. The registration function communicates with Sunbelt and your registration is processed. The information field at the bottom of the window details iHateSpam's registration status. The Number Of Seats is synonymous with the number of Exchange user mailboxes you pay for when you buy the software. Each "seat" equals an Exchange Mailbox. If you're running iHateSpam in Trial Mode and the trial period expires, mail passes through to the users normally—without filtering. Once you register, filtering kicks back in as previously configured.

Spam Filtering

Finally, we get to the business end of this spam fighter. iHateSpam blocks and filters spam globally and locally (to the user) with the following functions: whitelists/blacklists, blocked character sets, and weighted word filters. All of these functions are configurable for all users via the global filters or for individual users (or groups of users) with policies. These configuration options are available from the Spam Filtering management window. We discuss each option in the following sections.

General Settings The General Settings window allows you to enable/disable Bounce Message Filtering and enable/disable X-Header tags to nonspam. You may also update iHateSpam's global filtering definitions from this window.

iHateSpam Isn't Filtering!

Panic! The trial version expired, I registered it, and the software did not begin filtering!

Relax! Go to the Smart Caching window under Systems Management, and click the Clear SmartCache Contents button. Everything should work as before.

The Bounce Message Filtering flag allows (or disallows) bounced messages through the filter without processing. Thus, if for some reason one of your users receives a bounce message from a mailer-daemon or postmaster (for example, if a message was sent to a nonexistent e-mail address), iHateMail would let this message through without attempting to filter it. The filter engine processes bounce messages normally if this feature is disabled.

NOTE You'll probably want to filter bounce messages, since forging these messages is a well-known spammer tactic. The downside is that if a legitimate bounce gets filtered, it will make undelivered mail more difficult for you to troubleshoot.

The Spam Definitions tool allows you to update iHateSpam's global filtering definitions manually from Sunbelt Software's central server. Since these updates occur quite frequently, you'll want to configure automatic updates. (See the sidebar titled "Scheduling Automatic Updates with Windows Scheduled Tasks.") If you update the definitions, be sure to clear the Smart Cache for the settings to take effect immediately.

Scheduling Automatic Updates with Windows Scheduled Tasks

Although no tool is available for configuring automatic definition updates, the task is easy to do using the Windows Scheduled Tasks tool. To set up automatic updates, perform these steps:

1. Click the Start menu and navigate to Control Panel | Scheduled Tasks. Most Windows Server installations also launch the Scheduler automatically. The icon is located in the Windows system tray in the lower-right corner of the desktop.
2. Double-click the Add Scheduled Task icon. The Scheduled Task Wizard begins.
3. Click the Next button.
4. A list of available programs appears, but you'll probably have to browse to the file you want. The file you're looking for is GIANTSpamDefinitionsUpdater .exe located in the *$Programfilesroot*\Sunbelt Software\iHateSpam Server Edition\ folder. (*$Programfilesroot* is the directory where your program files are normally stored. Ours is C:\Program Files.)
5. Once located, double-click the filename. A Task window appears with the filename in the Program field and a series of radio buttons. Select Daily and click the Next button.
6. In the Time And Day window, select a start time (later the better, though it's not much of a resource hog), and select the Every radio button. Have the updater run every three days or so. Enter a desired start date (today is the default) and click the Next button.

Scheduling Automatic Updates with Windows Scheduled Tasks *(continued)*

7. Enter the Administrator user (or a user with Administrator privileges), enter and confirm the user's password, and then click the Next button.
8. Click the Finish button and the GiantSpamDefinitionsUpdater icon should appear in the Scheduled Tasks window. You're done.

Global Filters As stated previously, global filters affect all e-mail users managed by iHateSpam. These filters include Whitelist Rules, Blacklist Rules, Custom Rules, Character Set Blocking, and Filter Plug-ins.

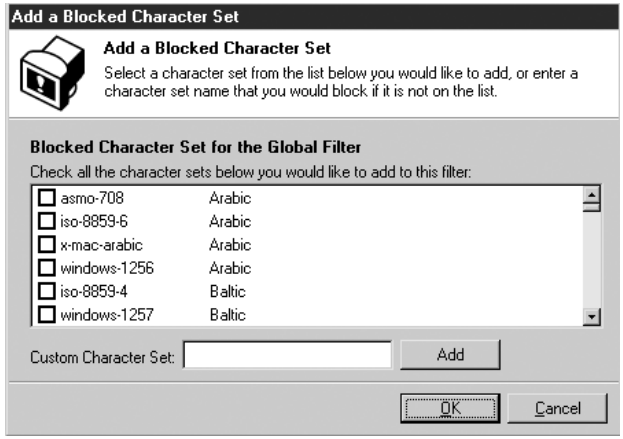
1. Click the Global Filters icon on the Spam Filtering management window to bring up an explanation of all the global filters.
2. First, we'll configure the Whitelist and Blacklist rules. Click the Whitelisted Senders folder in the left pane to open the Whitelist rules. You should see a Domain Address Type and sunbelt-software.com as a whitelisted E-mail Sender in the table in the right pane.
3. To add a whitelisted sender (either a full domain or an individual e-mail address), right-click anywhere on the table, and choose New | Whitelist Address. The Add An Allowed Sender window appears.
4. Select E-mail Address or Domain from the drop-down list and type the appropriate address into the field provided.
5. When you're done, click the OK button. The e-mail address or domain is added to the whitelist and allowed through the filter with almost no processing.

NOTE The Blacklisted Sender window works exactly the same way, except, of course, those domains and users are blocked.

CAUTION While the sample whitelist setting allowing any mail from sunbelt-software.com to pass your filtering process is fine for the sake of illustration here, you'll want to delete that whitelist entry, since any spammer can forge the From field of a spam message as coming from the whitelisted domain. It's never a good idea to stick with default settings such as these, since this information is freely available to anyone.

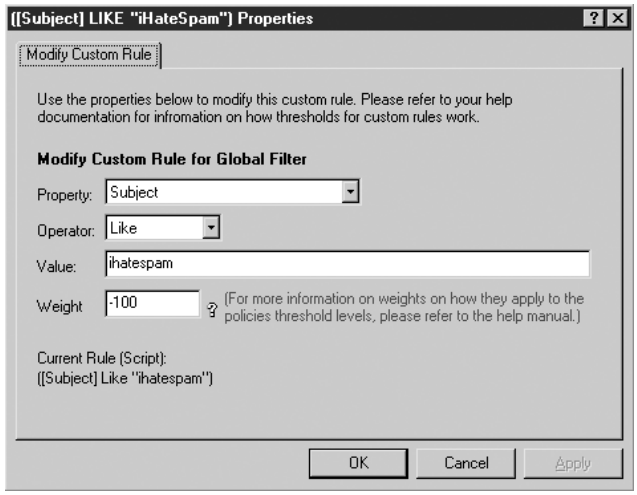
The Blocked Character Sets configuration automatically blocks any e-mail composed in whole or in part of the character sets designated. Thus, if you block all Arabic character sets, any e-mail iHateSpam processes composed in Arabic is automatically blocked. To add or

remove character set blocks, right-click the Blocked Character Sets folder in the Global Settings tree, choose New | Blocked Character Sets. The Add A Blocked Character Set window appears, as shown here. Simply check the checkbox next to the character sets you wish to block (or uncheck those to unblock) and click the OK button. The blocked character sets should appear in the right pane.


Add a Blocked Character Set
Add a Blocked Character Set
Select a character set from the list below you would like to add, or enter a character set name that you would block if it is not on the list.
Blocked Character Set for the Global Filter
Check all the character sets below you would like to add to this filter:
asmo-708 Arabic
iso-8859-6 Arabic
x-mac-arabic Arabic
windows-1256 Arabic
iso-8859-4 Baltic
windows-1257 Baltic
Custom Character Set:
Add
OK
Cancel

You may wish to create custom rules to apply to global definitions (as we did). To do this, simply click the Custom Filtering Rules folder in the Global Filters tree. The right pane of the management window displays current Custom Filtering Rules. By default, iHateSpam created its own custom filtering rule that fires on the word *ihatespam* and applies a –100 weight to that message (probably allowing it to pass through the filter). iHateSpam's rule "language" is simplistic compared to other tools, and we found it fairly constricting, although with several key rules applied in concert, we achieved a 92 percent accuracy rating during our limited testing.

First, let's look at iHateSpam's example rule. To view the rule, right-click it and choose Properties. The Properties window appears, as shown next. The Property drop-down menu allows you to select the area of the message you want iHateSpam to check, including the body, subject, sender, or receiver e-mail address, as well as Sender IP address and other header fields. The Operator drop-down menu has two options: Like and = (equals sign). The Like setting applies the word-matching function as a regular expression. The = operator matches the word exactly. The Value field holds the word you want iHateSpam to match on, and the Weight field applies the score entered (negative or positive) to any mail that matches the rule. Thus, this particular rule scans for *ihatespam* as a regular expression in the Subject field of incoming e-mails. If the value is found, iHateSpam applies a –100 weight to the mail. Depending on the other rules that fire on a particular message, the server either passes the message on or quarantines it.


([Subject] LIKE "iHateSpam") Properties
Modify Custom Rule
Use the properties below to modify this custom rule. Please refer to your help documentation for infromation on how thresholds for custom rules work.
Modify Custom Rule for Global Filter
Property: Subject
Operator: Like
Value: ihatespam
Weight -100
(For more information on weights on how they apply to the policies threshold levels, please refer to the help manual.)
Current Rule (Script):
([Subject] Like "ihatespam")
OK
Cancel
Apply

NOTE While this example rule is fine for illustration, you'll probably want to delete it from the Custom Filtering Rules window, since any spammer can figure out from the documentation, this book, or the iHateSpam program itself that a default rule applies a negative weight to the Value *ihatespam*, affording such a message a pretty good chance of getting through the filter.

To create a rule, right-click the Custom Filtering Rule folder and choose New | Custom Rule. The Properties window shown previously appears. Select the Properties you want iHateSpam to scan. To select multiple properties, hold down the CTRL key while you click. Select the Operator, input a value, and input a weight to apply to the mail. Click OK and the rule is added to the Filtering Rules table.

Policies Policies are used to apply Quarantine, Delete, and No Action Thresholds; set paths for quarantined mail; group whitelists or blacklists; and quarantine handling procedures. In addition, you can apply policy-specific Blocked Character Sets and Custom Filtering Rules. Policies are applied to individual users, although more than one user can utilize a given policy.

iHateSpam's Message Weighting System

The weighting system that iHateSpam uses is similar to those of other tools we've covered in this book. For each e-mail property that matches a given rule (global or policy), iHateSpam applies that value to the e-mail's "spam score." When all weights are applied, the numbers are added up and compared against the Quarantine and Delete Threshold (which is applied by Policies). If the mail is rated larger than one or both of these thresholds, iHateSpam handles it accordingly. If it's below the threshold, the mail goes on to the user's Inbox.

To access the Policies management window, click the Policies folder in the Spam Filtering tree. As with the Whitelist and Global Policy management windows, iHateSpam has a Default Policy, listed in the right pane of the management window. Right-click the Default Policy under the Policies tree and choose View | Customize. The right pane should populate with the Default Policy properties, as shown in Figure 11-9. The values in each field are modifiable and self-explanatory, though we'll cover Redirection and Policy Quarantine Actions next. No guidelines for threshold settings are available; these settings are a factor of what custom rules you're going to apply, what global custom rules are in effect, and the mix of spam to legitimate e-mail in your enterprise. The folder locations for Quarantine, Deleted, and Redirection are under the user's mailbox folder tree. The default policy places them in a root Spam folder and then a subfolder for each filter action.

NOTE Each folder name must end in a forward slash (/).

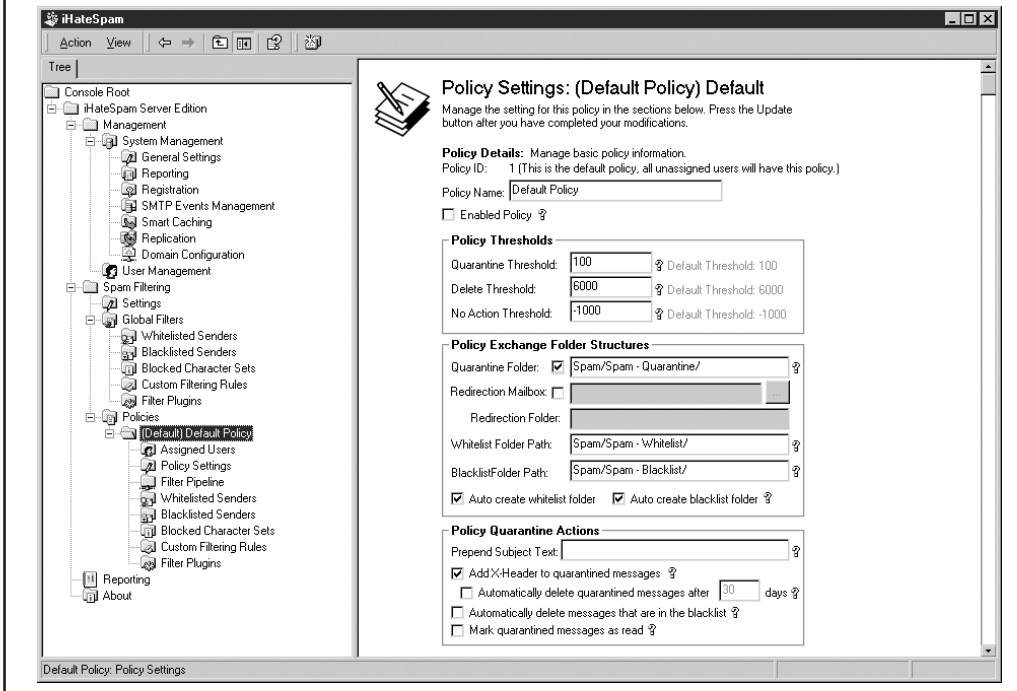


Figure 11-9. The Default Policy properties

The Redirection Mailbox function allows you to set up an e-mail box to direct all quarantined mail for a specific policy. This is useful if users do not want the bother of sifting through quarantined mail, or if the sheer volume of quarantined mail precludes downloading it to remote users. If you use this function, you'll definitely want to set the Automatically Delete Quarantined Messages After __ Days checkbox in the Policy Quarantine Actions section of the policy. This will prevent administrators from inadvertently forgetting to clear out this folder and causing a storage crisis.

The Policy Quarantine Actions section of the policy allows you to set custom Subject Text to prepend (add before) the actual subject of an incoming message, set an X-header (hidden header), and manage quarantined mail. This is useful if you are not using a Quarantine folder, but dumping all mail to the user's Inbox instead. If a message trips the quarantine threshold, your custom text is added to the Subject. The user can then set filters on the local mail client to sort these messages to local folders for later review. You can also add an X-header to the message that trips the quarantine threshold, also for the purposes of filtering at the client level. The X-header contains the weight applied to the message.

To add a new policy, right-click the Policies folder under the Spam Filtering tree in the management window and choose New | Create a Policy. The Create A New Policy Wizard window appears, as shown in Figure 11-10. Name the policy, set Policy Thresholds and Exchange Folder Structures as desired, and then click the OK button. The new Policy is added to the Policies tree.

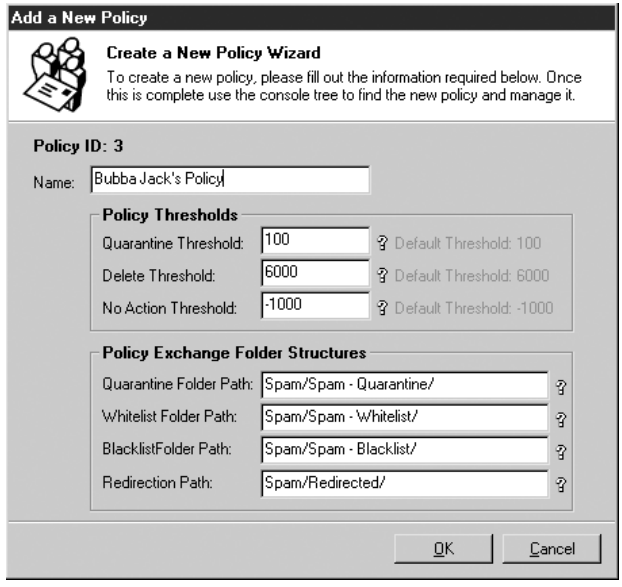
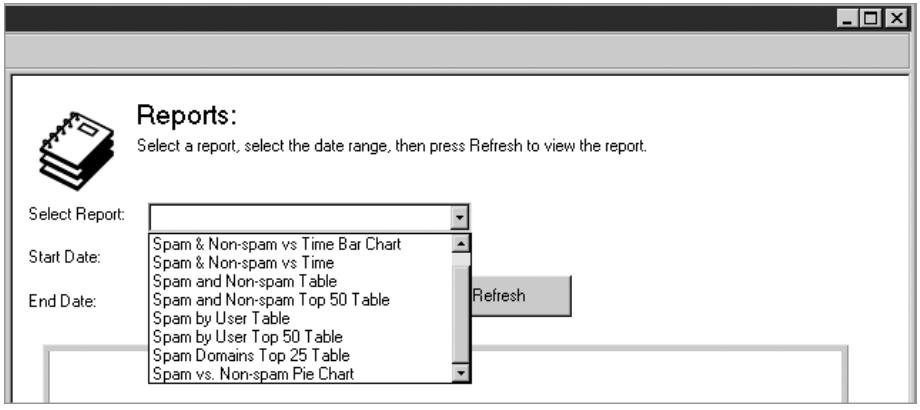


Figure 11-10. The Create A New Policy wizard

If you then click the + symbol next to your new policy folder in the management window, the tree expands with functions you'll recognize from previous sections. Here you can view, add to, or delete users from the policy (with the Assigned Users function), and view and change the Policy Settings, Whitelisted and Blacklisted Senders, Blocked Character Sets, and Custom Filtering Rules. All of these functions operate exactly as described earlier in this section. Remember that these settings are specific to this policy, only. After performing a major update, remember to reset the Smart Cache from the Smart Caching management window.

Reporting The Reporting tool allows you to generate iHateSpam default reports on various criteria. To access the Reporting tool, click the Reporting icon in the Management tree. The Reporting management window appears in the right pane, as shown here. We found the reporting to be well done, although no function is available for generating custom reports. To generate a report, select a report type, Start Date, and End Date from the drop-down lists provided and click the Refresh button. The report appears in the box provided. Although you cannot output reports from the management console, iHateSpam includes a stand-alone report viewer that allows for printing.


Reports:
Select a report, select the date range, then press Refresh to view the report.
Select Report:
Start Date:
End Date:
Spam & Non-spam vs Time Bar Chart
Spam & Non-spam vs Time
Spam and Non-spam Table
Spam and Non-spam Top 50 Table
Spam by User Table
Spam by User Top 50 Table
Spam Domains Top 25 Table
Spam vs. Non-spam Pie Chart
Refresh

GFI MAILESSENTIALS

MailEssentials is a Bayesian filter-based anti-spam server solution available from GFI, Inc. In addition to spam filtering, MailEssentials adds server-based e-mail tools such as global disclaimer signatures, reporting, mail archiving, and auto-replies.

How It Works

MailEssentials controls spam at the gateway by applying Bayesian rulesets, blacklists and whitelists, and other functions to all incoming mail. Like most Bayesian filter-based tools, MailEssentials learns the difference between spam and legitimate e-mail over time within your specific enterprise. MailEssentials filters scan each message in its entirety,

firing on keywords, checking for whitelisted/blacklisted domains and e-mail addresses, and verifying header information, such as domains, forged headers, mutation, and the like. Once the scan is done, it applies a weight to the message (its likely spam probability) and filters it according to thresholds that you set. In addition, MailEssentials checks third-party DNS blacklists, such as those discussed in Chapter 5 of this book. Messages tagged as spam can be deleted, forwarded to another address, or stored in customizable public or user folders. MailEssentials also provides features such as archiving all incoming and outgoing e-mail to a database, responding to spammers with a fake nondelivery report, and appending an organization-wide disclaimer to all outgoing e-mail. All of MailEssentials operations are logged and viewable from a reporting function.

Installing GFI MailEssentials

MailEssentials is available from the GFI web site at *http://www.gfi.com/mes/*. MailEssentials runs on a Windows 2000/2003 Server or Advanced Server with Microsoft Exchange 2000/2003. If you plan to use the MailEssentials reporter, Microsoft XML core services are also required (included with the install package). MailEssentials uses about 30MB of hard disk space and about 200MB of space for temporary files.

MailEssentials can be installed either on the Exchange server or on a separate machine. Though we cover only the first scenario here, the User Manual describes the installation and configuration procedures for running MailEssentials on a separate server.

Running MailEssentials on a separate server requires the following configuration:

- Windows 2000/2003 Professional or Advanced Server or Windows XP Professional
- Internet Information Server 5 SMTP service installed and running as an SMTP relay to your mail server
- Microsoft Exchange Server 2000, 2003, 4, 5, or 5.5; Lotus Notes 4.5 or higher; *or* an SMTP/POP3 mail server

Keep in mind that Windows 2000 and XP Professional accept only up to 10 incoming SMTP connections simultaneously; thus, if your organization uses e-mail more heavily than this, consider using Windows 2000 or 2003 Server or Advanced Server.

NOTE For more information about running MailEssentials as a separate server, refer to the User's Manual on the GFI support web site.

Preinstall Checklist

You don't have much to do prior to installing MailEssentials. Ensure that you have Administrator access to the Exchange server and enough disk space, and download the installation archive. Double-click the archive to extract it to a temporary folder and perform the steps in the following section to install.

Installing

To install MailEssentials on your Exchange 2000/2003 server, perform the following steps:

1. Double-click the Setup.exe file in the temporary folder where you extracted the archive. The Welcome Screen appears.
2. Click the Next button and in the Check For Latest Build window, select the Do Not Check For A Newer Build radio button. Then click the Next button.
3. Agree to the license agreement and click the Next button.
4. Select a destination folder and click the Next button.
5. Enter your name (or just enter **Administrator**), your company name, and the software serial number, if applicable. (If you are installing the MailEssentials Evaluation Version, *Evaluation* appears in the Serial Number field. Click the Next button. The Administrator Email window appears.
6. Enter an administrator's e-mail address in the field provided. This does not necessarily have to be the Exchange or Windows Administrator account. This is the person (or group) to contact when MailEssentials issues a critical notification. Once you're done, click the Next button.
7. The Active Directory window provides configuration options depending on your current mail server setup. If your Exchange server has access to all the users in the Active Directory (that is, it's not a front-end server for another Exchange server behind the network DMZ), select the Yes radio button. If this Exchange server doesn't have access to all mail users in the Active Directory, select the No radio button. This runs MailEssentials in SMTP mode. In Active Directory mode, MailEssentials can apply user-based rules and configurations to users automatically, while in SMTP mode, you must manually enter the users before applying user-based rules.
8. In the Ready To Install window, verify the information you've entered and click the Next button.

NOTE The Ready To Install window lists your local domain. MailEssentials can filter only on your local domain; thus, if this information is incorrect, no mail will be filtered. It pulls this information from your IIS setup, so if the information is wrong, check here first.

9. The program installs. About halfway through the install process, MailEssentials asks whether you want to restart the SMTP service. Click the Yes button to restart it. You'll see the "Success" window, where you can click Finished.

Configuring the Essentials

MailEssentials uses a centralized management console for most of its functions, though the GFI Monitor, Reporting, Troubleshooter, and the Bayesian Analysis Wizard are separate programs. To access the management console, click the Start button, point to Programs | GFI MailEssentials | MailEssentials Configuration. The standard Windows management console appears with a tree of functions in the left pane and a table in the right pane. The Anti-Spam tree contains all of the functions covered in this section, including Blacklist/Whitelist, Bayesian Analysis, Header Checking, and Keyword Checking.

Blacklists/Whitelists

Click the Blacklists/Whitelists icon in the Anti-Spam tree to access these functions. Click the Properties icon in the right pane to pull up the Blacklist/Whitelist Properties window, as shown in Figure 11-11. The Properties window allows you to configure the Whitelists (and auto-whitelisting feature), Blacklists, and DNS Blacklists, as well as perform actions on e-mail that's blocked by the Blacklists.

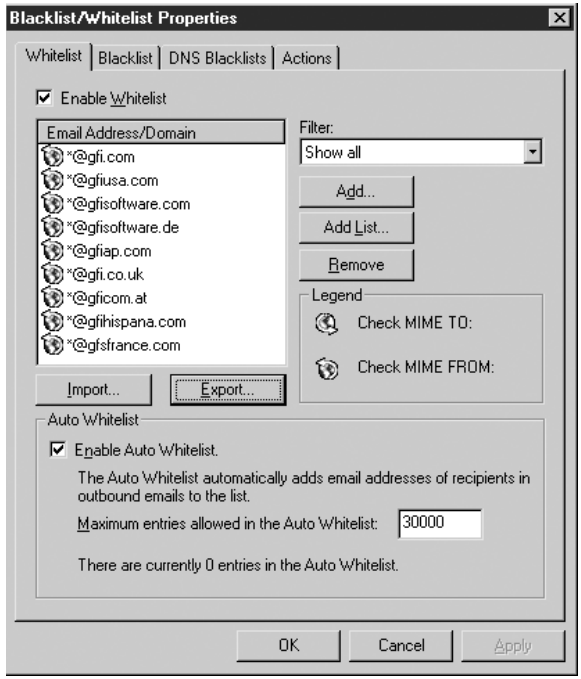


Figure 11-11. The Blacklist/Whitelist Properties window

Whitelists The Whitelist configuration window is similar to other tools covered in this book. Here you may add an e-mail address, domain name, and mailing list MIME To fields, and you can import and export the whitelist. Additionally, you can enable (or disable) the auto-whitelisting feature that automatically adds recipient e-mail addresses for all outbound e-mail. Enabling this feature should be approached with caution, however, especially if users in your organization periodically respond to spam mail (even if only to remove themselves from the spammer's list) or if your organization is plagued by e-mail viruses originating from known e-mail addresses.

To add a whitelist entry, click the Add button, type in the e-mail address or domain name, and then click the OK button. To add a domain, be sure to put *@ before the domain name (thus, to add the domain astk.tld, you would enter ***@astk.tld**). To add multiple "extended" domains, such as support.astk.tld, finance.astk.tld, and so on, you would simply enter ***@*.astk.tld**. Note that GFI has included GFI-related domain names on the whitelist. These should be removed, unless you have a specific reason for adding them to your organization's whitelist. The Add List button allows you to add the newsletter/notice/mailing list e-mail addresses and domains found, not in the From field, but in the MIME To field of the message headers. Entry in the Add List window is the same as previously explained.

Blacklists The Blacklists tab of the Properties window allows you to add domains and e-mail addresses you want to block automatically. Entering the information is similar to entering information in the Whitelist tab, although you can choose for MailEssentials to check the MIME To or MIME From field of the e-mail headers for the appropriate address or domain. You may also import from or export to an XML file containing e-mail addresses and domains.

DNS Blacklists The DNS Blacklists tab of the Properties window allows you to configure MailEssentials to check up to two DNS Blacklist services. Simply check the appropriate checkboxes and select the services you wish to use from the drop-downs provided. Note that if you select two DNS Blacklists, they must select different services from each drop-down list. More information about DNS Blacklists can be found in Chapter 5 of this book.

Actions The Actions tab of the Properties window allows you to configure what MailEssentials does with e-mail that triggers the local blacklist and the DNS Blacklist features. You may select one of the following actions:

- **Delete** Deletes the mail automatically.
- **Forward To User's Spam Folder** Puts the e-mail in the user's spam folder that you specify.
- **Forward To An Email Address** Allows you to forward the blocked mail to any e-mail address.
- **Move To A Specified Folder** Moves the mail to a folder on the server.

You can also tag the blocked e-mail with a definable word or phrase (prepended to the subject of the message) for handling after it reaches its destination. Logging of blacklist hits is configured from this window, as well as nondelivery reports generated to the spammers that find themselves on the blacklist.

Bayesian Analysis

To access the Bayesian Analysis Properties window (Figure 11-12), click the Bayesian Analysis icon in the Anti-Spam tree, and then click the Properties icon in the right pane of the management console. This window has only two tabs: General and Actions.

The General tab allows you to enable/disable Bayesian Analysis by clicking the respective checkbox. The Learning Updates Options section allows you to enable/disable Automatic Learning based on outgoing e-mails. This feature builds a stronger Bayesian filter, since MailEssentials learns keywords and phrases used in your organization's e-mail communications, likely good e-mail addresses and domains, and other information. You can also update your spam filter database from GFI's central servers by clicking the Download button. GFI updates these filters every few weeks.

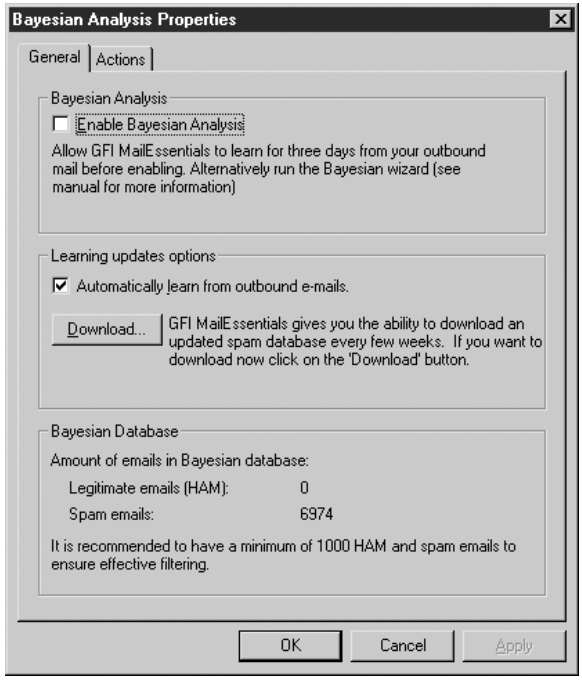

Bayesian Analysis Properties
General
Actions
Bayesian Analysis
Enable Bayesian Analysis
Allow GFI MailEssentials to learn for three days from your outbound mail before enabling. Alternatively run the Bayesian wizard (see manual for more information)
Learning updates options
Automatically learn from outbound e-mails.
Download...
GFI MailEssentials gives you the ability to download an updated spam database every few weeks. If you want to download now click on the 'Download' button.
Bayesian Database
Amount of emails in Bayesian database:
Legitimate emails (HAM): 0
Spam emails: 6974
It is recommended to have a minimum of 1000 HAM and spam emails to ensure effective filtering.
OK
Cancel
Apply

Figure 11-12. The Bayesian Analysis Properties window

The bottom section of this window gives you information on the Bayesian database. This information details the number of legitimate and spam e-mails the filter has processed and learned from. As stated in this window, MailEssentials needs about 1000 each of legitimate and spam mails to ensure effective filtering.

MailEssentials is essentially "dumb" out-of-the-box, so you have one of two options to start using the program immediately. Either use the outbound learning configuration option or download "spam knowledge" from GFI's web site. While either method works, the second is faster, since it may take a couple of days for enough outgoing mail to teach MailEssentials. Of course, learning what spam is to your organization is possible only by examining the e-mail received on your mail server.

The Actions tab is much like the Actions tab in the Whitelist/Blacklist Properties window. Here you can specify precisely what you want done with messages believed to be spam: delete, forward to a user's folder, forward to an e-mail address, or move to a local folder. You can also tag the message, enable the log file, and enable nondelivery messages, as described previously.

Header Checking

From the Header Checking configuration window, you can specify certain header checks that can assist MailEssentials spam profiling operations including MIME header fields scanning, DNS lookups, character set blocking, and handling actions. To access the Header Checking Properties window shown in Figure 11-13, click the Header Checking icon in the Anti-Spam tree, and then click the Properties icon in the right-hand pane of the management console.

General Settings The General tab of the Header Checking Properties window allows you to configure specific checks on MIME and SMTP fields in an incoming e-mail message's headers. Using the General and General Contd. tabs' checkboxes, you can configure MailEssentials to check the following information:

- **MIME From:** This checks to see whether the sender has configured an e-mail address in the mail client.
- **Malformed MIME From:** This check verifies that the MIME From field matches the specifications of RFC 822.
- **Maximum number of recipients** Though currently this is rarely an indication of spam, you can set the maximum number of recipients on a given e-mail. This is useful if you have internal or external "annoyance" spammers that send joke lists or chain e-mails, or that tend to reply to all recipients on a bandwidth-chewing e-mail thread that just won't die.
- **SMTP To: and MIME To: comparison** This setting compares the two settings in a given message and kicks out those that don't match. Of course, e-mail list servers often fit this profile, so if your organization subscribes to e-mail discussion lists, newsletters, and the like, be sure to add the e-mail address or domain name to the whitelist if you enable this feature.

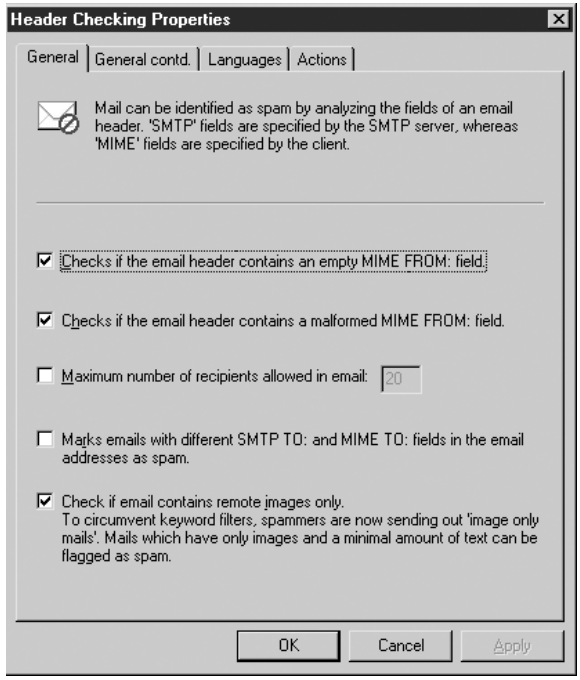

Header Checking Properties
General
General contd.
Languages
Actions
Mail can be identified as spam by analyzing the fields of an email header. 'SMTP' fields are specified by the SMTP server, whereas 'MIME' fields are specified by the client.
Checks if the email header contains an empty MIME FROM: field.
Checks if the email header contains a malformed MIME FROM: field.
Maximum number of recipients allowed in email:
20
Marks emails with different SMTP TO: and MIME TO: fields in the email addresses as spam.
Check if email contains remote images only.
To circumvent keyword filters, spammers are now sending out 'image only mails'. Mails which have only images and a minimal amount of text can be flagged as spam.
OK
Cancel
Apply

Figure 11-13. The Header Checking Properties window

- **Remote images** To combat a fairly new spammer tactic, this setting flags e-mails that contain only an image or an image with little text in the body of the e-mail. The drawback to this setting is that if your users often receive image files attached to e-mail messages, this could cause problems.
- **Domain validation** This setting is on the General Contd. tab. MailEssentials can look up the domain of an incoming message to verify that it's real and flag the message if it's not. The drawback is that the network overhead necessary to accomplish this may be excessive. Depending on e-mail volume, this could slow down both mail processing and spam filtering.
- **MIME from number limit**s A wily spammer tactic is to auto-generate a unique e-mail name (anything before the @ sign) to thwart blacklists. These generated names often contain numbers. Enable this feature and enter the threshold of numbers an e-mail name can contain before it's flagged.
- **Subject checking** This feature checks to see whether the Subject field of the message contains your name or e-mail name. Often spammers generate

"personalized" subjects from the recipient's e-mail address. Many e-mail administrators have received a message with the subject, "PostMaster, you're not going to believe this!" You can also add e-mail addresses to "Except" this rule, in cases where you often receive e-mails from legitimate sources that fit this profile.

Languages and Actions The Languages tab of the Header Checking Properties window allows you to specify lists of character sets (other languages) to block or not block automatically. To enable, click the Block Mails That Use These Languages checkbox and select either Block The List Below or Block All Except The List Below, and then select the character sets accordingly.

The Actions tab performs the same functions as the Actions tabs in the previous configuration windows: It blocks e-mails that fit the criteria set in this Properties window and either deletes, forwards to a user folder, forwards to an e-mail address, or moves the message to a local folder. You can also enable the Tag e-mail function, enable logging of events that meet this Properties' window configurations, and generate a fake non-delivery e-mail to the spammer.

Keyword Checking

In addition to the other header and list checks we've covered, MailEssentials also uses a complicated, yet easy-to-configure Keyword Checking function to identify spam. You can scan keywords or combinations of keywords in the message body or subject. To access the Keyword Checking Properties window shown in Figure 11-14, click the Keyword Checking icon in the Anti-Spam tree, and then click the Properties icon in the right pane of the management console.

The General tab contains the Scan Email Body table of keywords. It offers a sizable list of keyword and keyword combinations by default, but to add a keyword, click the Add Keyword button. In the text box, type the word or phrase you want MailEssentials to scan for, and then click OK.

MIME Fields in the Message Header

In a message header, MIME fields are generated by an e-mail sender's mail client, while SMTP fields are specified by the SMTP server through which the message passes. An example of a MIME field is the From field, designating the e-mail address of the sender, as configured by the sender's e-mail client. The Received field is an example of an SMTP generated e-mail header field. Note that MIME fields are not reliable sources of spam indication by themselves. For example, a misconfigured e-mail client (such as one without a name in the Name field), mail to multiple e-mail accounts (such as a legitimate mailing list), and the like could cause one of these rules to fire. Use them with care.

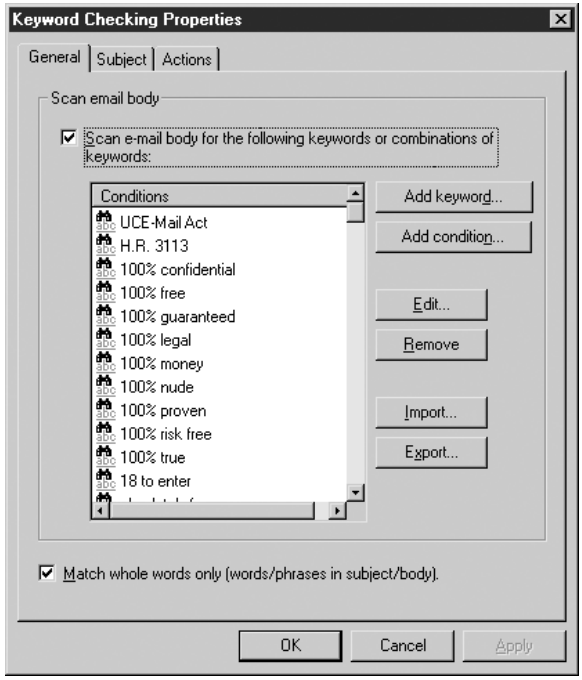
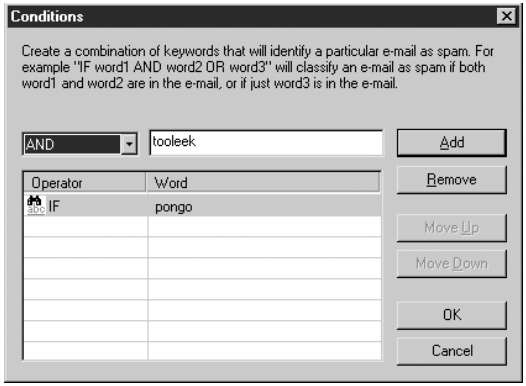


Figure 11-14. The Keyword Checking Properties window

You may also add a *condition*, which is a series of keywords linked by the operands *OR*, *AND*, *AND NOT*, and *OR NOT*. To access the Conditions window shown here, click the Add Condition button in the General tab. Type a keyword into the field provided, and then click the Add button. The keyword appears in the table with the operator *IF* beside it. Continue building the condition with the appropriate operators.


Conditions
Create a combination of keywords that will identify a particular e-mail as spam. For example "IF word1 AND word2 OR word3" will classify an e-mail as spam if both word1 and word2 are in the e-mail, or if just word3 is in the e-mail.
AND
tooleek
Add
Operator
Word
IF
pongo
Remove
Move Up
Move Down
OK
Cancel

The Subject tab allows you to add subject keywords and conditions and operates exactly the same as the body keyword/condition function. The Actions tab operates the same as the Actions tabs on the other Properties windows in this section, allowing you to block e-mail that meets the conditions on the Keyword Checking Properties configuration and either delete the message, forward it to the user's spam folder, forward the message to an e-mail address, or move it to a local folder. You can also tag the message with a word or phrase, enable logging of keyword events, and generate a fake nondelivery message back to the spammer.

Other E-Mail Functions

MailEssentials contains several other e-mail management utilities, including Mail Archiving and Mail Monitoring, as well as Auto-Reply and Global Disclaimer generation. Although these functions are outside the scope of this chapter, be aware that GFI has packed this anti-spam tool with a lot of functionality. For more information about these functions, refer to the MailEssentials User Guide and other documentation on the GFI web site.

TREND MICRO SPAM PREVENTION SERVICE

Spam Prevention Service (SPS) is a feature-rich spam-fighting tool from Trend Micro. Although its spam-filtering process is similar to that of other tools covered in this chapter, its deployment strategy is different. SPS fights spam as a pass-through SMTP server, meaning that instead of applying rules to e-mail already received by the mail server, SPS filters mail before it ever touches the mail server.

How It Works

Deployed between the mail server and the Internet, SPS assigns a numeric value to incoming e-mail based on an equation formed by rules that apply a spam score or weight to the incoming message. The spam score is then compared to a global threshold and the mail is either forwarded on to the mail server, tagged as spam and forwarded on, held on the SPS server, or deleted entirely. SPS runs on its own machine and monitors port 25 (the SMTP port). In addition to its complex filter set, SPS also filters mail using the standard whitelist/blacklist features and limited header scanning.

Installing SPS

SPS is available via CD or as an installation archive from the Trend Micro web site at *http://www.trendmicro.com*. Though Trend Micro also distributes SPS for Linux and Solaris, we cover the Windows 2000 Server version in this chapter. SPS should be installed on its own machine with at least the following specifications:

- 1GHz Intel Pentium 4 processor
- 512MB RAM

- 100MB of hard disk space for software only (logging and reporting require more space, though how much space depends on the volume of e-mail you receive and your configuration choices)

While several different deployment options exist, especially in conjunction with other Trend Micro products, we cover only the most basic SPS setup in this chapter: one SPS server and one e-mail server.

Preinstall Checklist

Before you can install SPS, make sure that a port is available for SPS to listen on and that the port is reachable through the firewall. The default port is 25 (SMTP port). You'll also want to have Administrator access to the computer where SPS is to be installed, as well as the ability to change the mail exchanger (MX) records on the mail server. The MX records should be changed to point to the SPS server for mail exchange.

Once you have all this under control, you're ready to install Spam Prevention Services.

Installing

Log in to the Windows 2000 server as a user with Administrator rights and perform the following steps to install SPS:

1. Disable any services running on port 25, even if you plan to run SPS on a different port. By default, SPS installs listening to port 25, and if another service is running on that port the installation process fails.
2. Double-click the install archive and follow the prompts to install SPS. No complex configuration options are required during the install process. You will agree to a license agreement, set a destination folder, and that's it.

Initial Configuration

Once the install process completes, open the SPS configuration window, shown in Figure 11-15 by navigating to Start | Programs | Trend Micro | TrendSPS.

The following configuration tabs hold all the SPS goodness: Configuration, Spam Filters, Exception Filters, ActiveUpdate, Report, and Log. The two big icons in the upper-left corner of the Configuration window start and stop the SPS service. The big message that appears at the top of the window always tells you the state of the service.

Configuration The Configuration tab allows you to configure receiving e-mail servers, trusted domains, the whitelist and blacklist, the IPLOCK feature, as well as Advanced configuration options.

The Receiving Email Servers setting controls where SPS routes the incoming mail when it's through filtering it. Click the Edit button and enter either an IP address or the fully qualified domain name of your mail server.

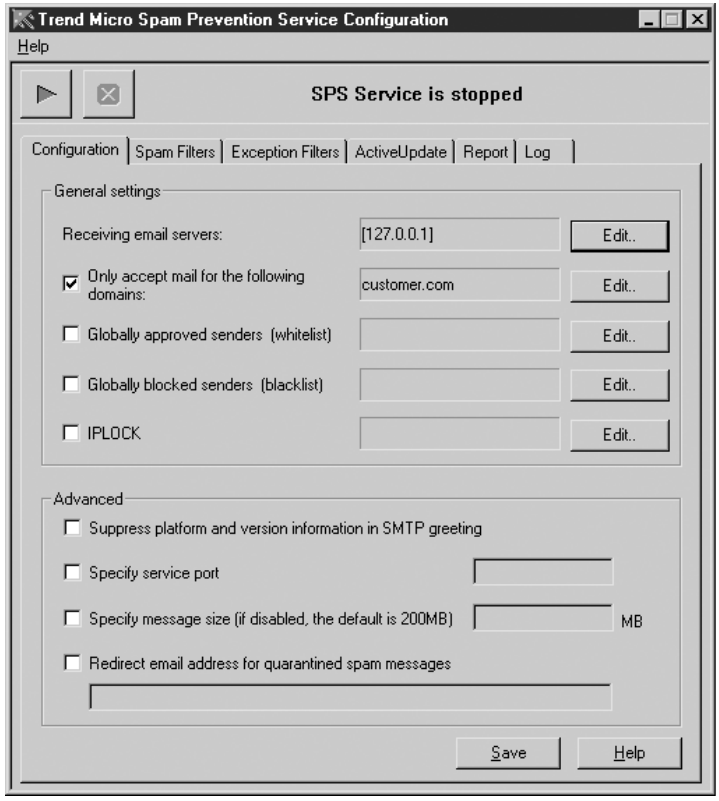


Figure 11-15. The SPS Configuration window

To enter an IP address, perform the following steps:

1. Click the Edit button.
2. In the field provided on the Receiving Email Servers window, enter the IP address enclosed in brackets (for example, [10.10.10.1]).
3. Click the Add button and the IP appears in the list provided.

To enter a domain name, perform the following steps:

1. Click the Edit button.

2. In the field provided on the Receiving Email Servers window, enter the full qualified domain name (with no brackets—for example, *mail.myserver.tld*).
3. Click the Add button and the domain name appears in the list provided.

If mail is being routed to multiple servers, multiple entries must be separated by commas. If you wish to deliver mail to a port other than 25, append the port number to the IP address or domain name, separated by a colon (:), as shown in the following examples:

- IP Address: [10.10.10.1]:2525
- Domain Name: mail.myserver.tld:2525

The Blacklist and Whitelist features allow you to add domains, IP addresses, and classless interdomain routing (CIDR) ranges of IP addresses in the formats shown next:

- Domain name: @spamhead.com
- IP address: [10.10.10.1]
- CIDR range: [10.10.10.0/12]

To include more than one entry, separate each with a comma. You can add up to 1500 blacklist and 1500 whitelist entries.

The IPLOCK feature prevents sender address spoofing (a common spammer tactic of low-grade identity theft). To enable IPLOCK, enter a domain name with an IP address or range. SPS then checks to see whether the IP address of the sender matches the range of IP addresses for the sender's domain. This setting is most useful if the spammer is attempting to spoof your domain name or one commonly used by legitimate senders to your mail server.

Other advanced features on this tab include these:

- **Specify Service Port** Configures SPS to listen for incoming mail on an alternative port (other than 25, the default).
- **Redirect Email Address For Quarantine Spam Messages** Lets you enter an e-mail address or addresses to which you will send quarantined messages.
- **Check Message Size** Directs SPS to check the size of incoming e-mails and tag those that exceed the size threshold as spam.

Spam Filters The Spam Filters tab, shown in Figure 11-16, allows you to configure (you guessed it) the SPS spam filters' sensitivity. Four category filters and one general spam level are available. These sliders control the actual thresholds to which SPS compares the weighted e-mail messages. To set the sensitivity level, simply slide the sliders on each filter left for less sensitive or right for more sensitive.

- **General Spam Level** This threshold is the base or bulk filter for all e-mail that passes through SPS.
- **Sexual Content** All word triggers associated with sexual content increase the message's Sexual Content value. This threshold controls whether a message is filtered or not.
- **"Make Money Fast"** Another of the Big Four spam messages. This filter has the potential to keep you poor but also spam free.

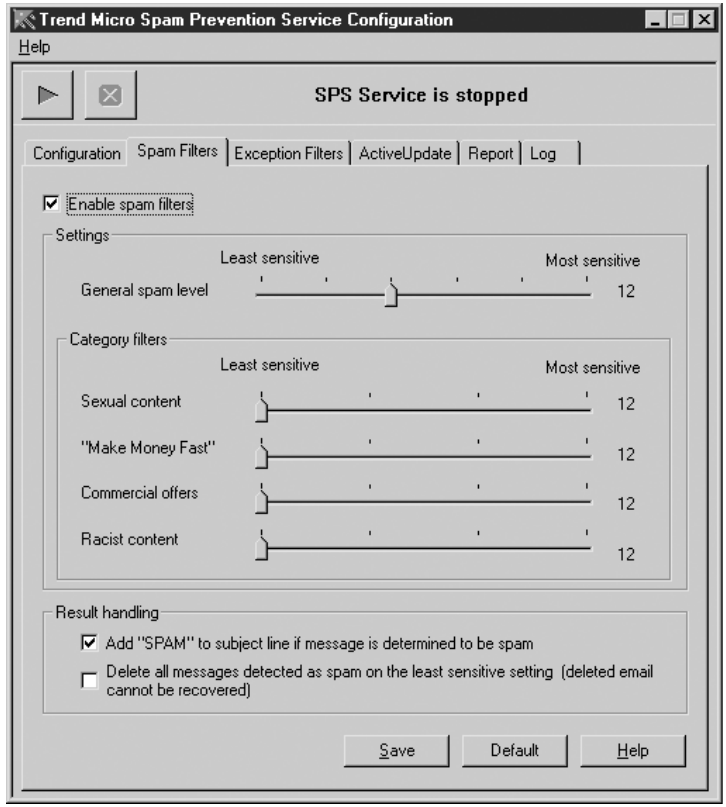


Figure 11-16. The Spam Filters tab

- **Commercial Offers** A catchall filter for advertisements of any kind other than the mentioned three. If you're a socialist, set this really high. To support capitalism, set this very low.
- **Racist Content** Though not exactly a common spam criteria, racially charged spam could land an organization in deep legal trouble.

The Spam Filters configuration window also allows you to add the word *SPAM* to the subject line of messages determined to be spam and to delete all messages detected as spam, by simply checking the appropriate boxes.

NOTE The SPS documentation contains a lengthy description of filter sensitivity and a great testing methodology for balancing sensitivity to performance. Refer to the SPS User's Guide on the Trend Micro web site for more information.

Exception Filters Exception filters allow you to configure filters to identify specific text strings (case-sensitive or insensitive) and immediately do something with that incoming message—be it delete, quarantine in a specific category, respond to the sender with an Error 50, or pass the message through. The most obvious use for this feature is as a "verification" method for legitimate e-mail. If your organization receives a lot of messages with the same text string (such as a disclaimer, message signature, and the like), configuring that string and setting the filter to pass-through diminishes the probability that the message will be misidentified as spam. Likewise, if you see spam messages that use the same string of text over and over and for some reason SPS is not catching these mails, simply set up an exception filter to find that string and automatically delete or quarantine the offending messages. It is important to note that using literal string matching with the body of a message can create numerous false negative scenarios.

To set up an exception filter, click the Exception Filters tab and click the New button. A text field appears for the name of the filter. Enter a name and click the OK button. The Exception Filter Editor window appears, as shown in Figure 11-17. Select an area of the message to scan for the string pattern (all the headers, various header areas, and areas of the body), enter the string to search for, and select either the Case Sensitive Match or Case Insensitive Match radio button. Then select an action for SPS to perform when it finds this string in a message. Once done, click the OK button and the exception filter is added to the list.

Updates, Logs, and Reports SPS uses three main utilities to track, update, and report on its spam-fighting activities. To set up SPS for automatic updates, simply click the ActiveUpdate tab, enable the scheduled update process, and set a time and frequency to check for updates. If you're on a network with a proxy server, you can configure that from this window, as well.

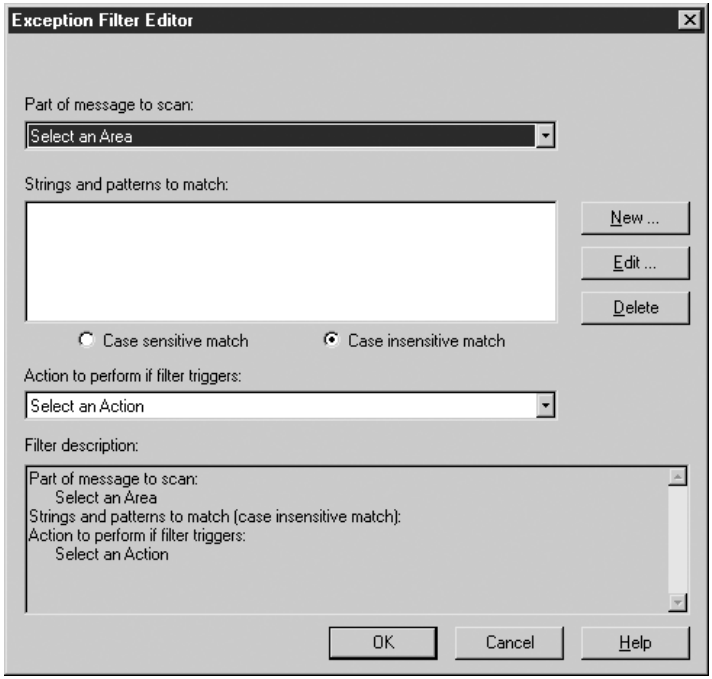


Figure 11-17. The Exception Filter Editor window

Finally, the Report tab allows you to construct various reports of SPS's activities over time and output that report either to text or HTML format. The Log tab provides a configuration interface to set up rotating log files of SPS's activities. You can either manually rotate logs by clicking the Rotate Now button or set up a schedule for SPS to rotate its log files automatically.